Tech Note 1055 Enabling OPC UA Discovery and Encryption

All Tech Notes, Tech Alerts and KBCD documents and software are provided "as is" without warranty of any kind. See the Terms of Use for more information.

Topic#: t002900 Created: October 2014

Introduction

OPC UA Encryption allows for more secure, certificate-based, communications.

You can use OPC UA Discovery to allow you to browse for available OPC UA Servers, simplifying OPC UA Configuration.

Application Versions

• ArchestrA OPC UA Client Service v1.0

Assumptions

This Tech Note assumes you have already installed the following prerequisites:

- Application Server 2014 P01 or later
- ArchestrA OPC UA Client Service v1.0 or better
- Any 3rd party OPC UA Server
- We will use TOPServer 5.x and its simulation driver for this example

Prepare the System

1. In Windows Explorer, show hidden files and folders.



FIGURE 1: SHOW HIDDEN FOLDERS

 Download and install OPC UA SDK Sample Applications v1.02 from the OPC Foundation (http://www.opcfoundation.org). It is located under Developer Tools - Developer Kits - Unified Architecture - Sample Applications: Direct link: https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/sample-applications.

Create an ASB OPCUA Client Service Instance

Create an ASB OPCUA Client Service instance in the IDE (this generates the required client certificate).

1. Click Galaxy>Configure>ArchestrA Services.



FIGURE 2: CONFIGURING ARCHESTRA SERVICES

2. Right-click ASBOPCUAClientService and choose Create.



file:///C|/inetpub/wwwroot/t002900/t002900.htm[10/15/2014 8:05:56 AM]

FIGURE 3: CREATING AN ASB OPC UA CLIENT SERVICE INSTANCE

Configure OPC UA Server Security Settings

- 1. From the Start menu, click Start>All Programs>Software ToolBox>Top Server5>OPC UA Configuration.
- 2. Click on Server Endpoints tab.
- 3. Enable or create a Server endpoint that uses the computer node name.
- 4. Set your desired encryption method (Basic256, Sign & Encrypt in this case).

OPC UA Configurati	on Manager	x
Server Endpoints Trus	ted Clients Discovery Servers Trusted Servers	Instance Certificates
URL	△ Security	
🦗 opc.tcp://127.0.	0.1:49380 Basic128Rsa15	(S,SE), Basic256 (S,SE)
opc.tcp://DS-W0	R2-test:49380 Basic128Rsa15 ((S,SE), Basic256 (S,SE)
E	idpoint Definition	X
	TCP Connection	
	Network Adapter: Default	_
	Port Number: 49380	
	opc.tcp://DS-W08R2-test:4	49380
	Security Policies	
	None	
Enabled	Basic128Rsa15 Sign; Sign and Encry	ypt 💌
Add	Basic256 Sign and Encrypt	
ote: Server Runtime	ОК	Cancel Help elp

FIGURE 4: CHOOSE SERVER-SIDE ENCRYPTION

5. Click the **Trusted Clients** tab and import the ArchestrA OPC UA Client Service Certificate from: C:\ProgramData\ArchestrA\CertificateStores\OPCUAClient\certs\aaUAClient.def.

Clent name	UR	રા		
TOP Server/UA Client	Driver un	n:DS-W08R2-test:SWToolbox.	TOPServer.V5:UA	
	Import Certificate			
	GO C: ProgramD	ata\ArchestrA\CertificateStore	es (OPCUAClient \certs) 💌 🗱 Search certs	s
	Organize • New folder			· • 🖬 (
	Favorites	Name ~	Date modified	Type
	E Desktop	aaUAClient	3/27/2014 9:41 PM	Security Certificate
Import Export. :: Server Runtime reinitia	Computer Compu			
	Setwork -	•		

FIGURE 5: DEFINE TRUSTED CLIENTS

- 6. Click the **Discovery Server** tab.
- 7. Import the Discovery Server certs from: C:\Program Data\OPC Foundation\UA\Discovery\pki\own\ualdscert.der.

Server Name	A U	a		
	Import Certificate			
	GO C:\ProgramD	ata\OPC Foundation\UA\Discovery\pki\own	💌 🔛 Search own	
	Organize 👻 New folder			· · 🖬 (
	Favorites	Name *	Date modified	Туре
	E Desktop	ualdscert	8/8/2014 1:52 PM	Security Certificate
Import Remo	Recent Places Concurrents Concurrents Concurrents Computer Computer Concurrents Concurren			
	C DVD Drive (D:) SQL			

FIGURE 6: LINK OPC UA SERVER TO DISCOVERY SERVER

- 8. Click the Instance Certificates tab.
- 9. Export the Server Certificate to a temporary location like Documents and give it a name with a '.der' extension



FIGURE 7: EXPORT SERVER CERTIFICATE

- 10. Close the OPC UA Configuration Manager.
- 11. Reinitialize TOPServer Runtime for changes to take effect.

Configure OPC UA Discovery Security

- 1. Open the OPC Foundation OPC UA Configuration Tool (Start>All Programs>OPC Foundation>Unified Architecture>1.02>Sample Applications>Configuration Tool).
- 2. Click the Manage Certificates tab.
- 3. Select the **Directory Store %CommonApplicationData%\OPC Foundation\CertificateStores\MachineDefault** Store Path.

File Help						
Manage Security	Manage Application	Manage Certificates	Manage COM Interop	HTTP Access Rules		
Store Type	Directory	-				
Store (jpo						
Store Path	Common Application	nData%\OPC Foundation	on \Certificate Stores \Ma	chineDefault	•	Browse

FIGURE 8: CHOOSE CERTIFICATE STORE

- 4. Press the Import Certificate to Store button.
- 5. Browse to C:\Program Data\OPC Foundation\UA\Discovery\pki\own\ualdscert.der, and click Open to confirm.



FIGURE 9: IMPORT DISCOVERY SERVER CERTIFICATE

6. Click **Yes** to accept the Certificate.



FIGURE 10: ACCEPT THE CERTIFICATE

- 7. In the OPC Foundation OPC UA Configuration Manager, click the Manage Security tab.
- 8. Choose Application to Manage OPC.UA.DiscoveryServer and press Edit.

WA Configuration Tool				
File Help				
Manage Security Manage Application	Manage Certificates Manage COM Interop HTTP Access Rules			
Application To Manage Opc. Ua.D	scoveryServer	•	Find	Edt
	· · · · · · · · · · · · · · · · · · ·			
Trust Another Application	Sets up a trust relationship with another application			
View Trusted Certificates	Displays the certificate trust list that is currently assigned to the application.			
Select Certificate to Trust	Copies a certificate from in existing trust list to the application trust list.			

FIGURE 11: SETUP DISCOVERY SERVER SECURITY

9. On the Certificate line, press Browse.

xecutable File	C:\Program Files (x86)\Common Files\OPC Foundation\UA\v1.0\Bin\Opc.Ua.DiscoveryServer.ex	Browse
onfiguration File		Browse
ertificate		Browse
rust List		Browse
rust List This dialog specifi	I es the location of the information needed to configure security for a UA application. The configuration the security for a UA application for one he much be the test of the design of the test of the design of the test of tes	n file is the file used by the appl

FIGURE 12: MODIFYING DISCOVERY SERVER APPLICATION

10. Choose the Directory Store Type and MachineDefault Store.

11. Select the UA Local Discovery Server certificate, and click OK.

Location							
Store Type	Directory	•					
Store Path	%CommonAp	plication Data?	OPC Founda	tion\CertificateStore	s\MachineDefault		-
Filters							-
Subject Name							_
Domain							_
lssuer Name							-
	1.0						
Certificate Type Has Private Key	Applicatio	n 🖵 Certific	cate Authority	☐ Self-signed [Issued by CA		
Certificate Type Has Private Key Name	Applicatio	n T Certific	Private Key	C Self-signed C	Issued by CA	Valid Until	
Certificate Type Has Private Key Name UA Configurat	Applicatio F tion Tool	n Certific Type End-Entity	Private Key Yes	Domains DS-W08R2-TEST	Un U	Valid Until 2039-04-02	
Certificate Type Has Private Key Name UA Configurat UA Local Disc	Applicatio	n Certific Type End-Entity End-Entity	Private Key Yes No	Domains DS-W08R2-TEST DS-W08R2-TEST	Un Un Unsiocalhost:OPCFoundation:Configuration Tool um:DS-W08R2test:UALocalDiscoveryServer	Valid Until 2039-04-02 2017-08-10	

FIGURE 13: CHOOSE DISCOVERY SERVER CERTIFICATE

12. On the Trust List line, press Browse.

🛃 Modify Appli	cation Information	<u>_ ×</u>
Application Name	Opc.Ua.DiscoveryServer	
Executable File	C:\Program Files (x86)\Common Files\OPC Foundation\UA\v1.0\Bin\Opc.Ua.DiscoveryServer.exe	Browse
Configuration File		Browse
Certificate		Browse
Trust List		Browse
This dialog specifi store its security s is not known or it manage the conte	es the location of the information needed to configure security for a UA application. The configuration file ettings. This configuration file can be read by this tool if it conforms to the ApplicationConfiguration schem uses an unknown schema then the application certificate and trust list must be specified manually. Once ents of trust list.	is the file used by the application to a used by the OPC UA.NET SDK. If it this is done the tool can be used to
ок		Cancel

FIGURE 14: MODIFYING DISCOVERY SERVER APPLICATION

13. Select Windows Store Type, and path LocalMachine\UA Applications, then click OK.

Store Type	Windows		
Store Path	LocalMachine\UA Applications	I	Browse
014	1		C 1

FIGURE 15: CHOOSE WINDOWS CERTIFICATE STORE

14. Click **OK** to confirm your Application changes and click **Yes** to Overwrite.

🛃 Modify Applic	cation Information	
Application Name	Opc.Ua.DiscoveryServer	
Executable File	C:\Program Files (x86)\Common Files\OPC Foundation\UA\v1.0\Bin\Opc.Ua.DiscoveryServer.exe	Browse
Configuration File	[]	Browse
Certificate	DC=DS-W08R2-test, CN=UA Local Discovery Server, C=US, S=Arizona, L="16101 N. 82nd Street, Scottsdale", O=OPC Four	Browse
Trust List	[Windows]LocalMachine\UA Applications	Browse
This dialog specifi store its security so is not known or it o manage the conte	es the location of the information needed to configure security for a UA application. The configuration file is the file used by the app ettings. This configuration file can be read by this tool if it conforms to the ApplicationConfiguration schema used by the OPC UA. It uses an unknown schema then the application certificate and trust list must be specified manually. Once this is done the tool can b ints of trust list.	Dication to IET SDK. If it be used to
ок		Cancel

FIGURE 16: SAVE DISCOVERY SERVER APPLICATION CHANGES

15. Click the Manage Certificate tab and click the Windows Store Type and the path LocalMachine\UA Applications.

UA Configura	tion Tool		
File Help			
Manage Security	Manage Application	Manage Certificates Manage COM Interop HTTP Access Rules	
Store Type	Windows		
Store Path	LocalMachine\UA App	lications	Browse
CA Key File			Browse
View	w Certificates	Displays the certificates in the store.	
Create C	ertificate Authority	Creates a certificate that can be used to issue application certificates.	
Select an	d Issue Certificate	Selects an existing certificate and issues new one with the same information.	
1 1000		In a second second second	

FIGURE 17: MANAGE WINDOWS CERTIFICATE STORE CERTIFICATES

16. Select Import Certificate to Store.

17. Browse to the **Top Server** certificate that you exported earlier to My Documents and click **Open**.



FIGURE 18: IMPORT OPC UA SERVER CERTIFICATE TO THE WINDOWS CERTIFICATE STORE

18. Click Yes to accept the Import.



FIGURE 19: CONFIRM CERTIFICATE IMPORT

19. Click the Manage Security tab and with OPC.UA.DiscoveryServer selected, click Select Certificate to Trust.

File Help			
Ianage Security Manage Application	Manage Certificates Manage COM Interop HTTP Access Rules		
Application To Manage Opc.Ua.D	iscoveryServer	Find	Edit
Trust Another Application	Sets up a trust relationship with another application		
Trust Another Application View Trusted Certificates	Sets up a trust relationship with another application Displays the certificate trust list that is currently assigned to the application.		

FIGURE 20: EDIT DISCOVERY SERVER SECURITY

20. Select the **Windows** Store Type and the path **LocalMachine\UA Applications**, then select the TOPServer certificate and click **OK**.

Store Type	/indows	•				
Store Path	calMachine\U	A Applicat	ions			
Fiters						
Subject Name						
Domain						
Issuer Name						
Issuer Name	Application	Cettfi	cate Authorit	y ∏ Self-signed	☐ Issued by CA	
Issuer Name	Application	Cettfi	cate Authorit	y ∏ Self-signed	Issued by CA	
Issuer Name	Application	Certifi	cate Authorit	y T Self-signed	□ Issued by CA	Valid Until
Issuer Name Certificate Type C Has Private Key C Name TOP Server/UA	Application Ty Server" En	F Centri pe d-Entity	cate Authorit Private Key No	y Setf-signed	Lissued by CA Uni um:DS-W08R2test:SWToolbox.TOPServer.V5:UA Server	Valid Until 2024-04-14

FIGURE 21: SELECT SERVER CERTIFICATE TO TRUST

21. Click **OK** to acknowledge the Trust.



FIGURE 22: CONFIRM TRUST RELATIONSHIP

Configure the OPC UA Client Instance

1. In the IDE, right-click and check-out the ASB OPC UA Client Service instance.

-	P	tes	t		ASBO
		1	ASBOPCUAClientSer	vice	
	+ + +	44 44 44	ASBOPCUAClier ASBGRBrowsingSen ASBMxDataProvider ASBAuthenticationSe	Save Rename Delete Export	F2 Delete
				Create Copy	
				Check-out	
				Discard Check-out	
				Check-in	
				Override Check-out	
				Save And Check-in	
				Deploy UnDeploy	Ctrl+D Ctrl+U

FIGURE 23: CHECK-OUT ASB OPC UA CLIENT SERVICE INSTANCE

2. Give it a Scope Name of your choice.

ASBOPCUAClientService_001					
General OPC UA N	Seneral OPC UA Namespace				
Scope Name:	TOPServer				
- OPC UA Server Details -	Scope Name will be the Namespace in item references				

FIGURE 24: PROVIDE SCOPE NAME

3. Provide or browse for the OPC UA Server Node name.

ASBOPCUAClientService_001						
General OPC UA N	OPC UA Namespace					
Scope Name:	TOPServer					
	Scope Name will be the Namespace in item references					
OPC UA Server Details -						
OPC UA Server Node:	DS-W08R2-test					
Endpoint URL:	✓ 59					
Application URI:						

FIGURE 25: DEFINE OPC UA SERVER NODE

The Endpoint URL list populates when you press the drop-down and select your Endpoint URL.

ASBOPCUAClientService_001						
General	OPC UA N	amespace				
Scope Name	e:	TOPServer				
	Scope Name will be the Namespace in item references					
OPC UA Ser	rver Details –					
OPC UA Server Node:		DS-W08R2-test				
Endpoint U	IRL:	opc.tcp://DS-W08R2-test:49380				
Application	Application URI:					
- Security Me	Security Message Mode Security Policy					
None O Sign O Sign and Encrypt None O Basic256 O Basic128Rsa15						

FIGURE 26: CHOOSE OPC UA ENDPOINT URL

4. Set your Encryption to match the server.

ASBOPCUA	ClientServi	ce_001			
General	OPC UA N	amespace			
Scope Nam	e:	TOPServer			
	Scope Name will be the Namespace in item references				
COPC UA Se	rver Details –				
OPC UA Server Node:		DS-W08R2-test			
Endpoint URL:		opc.tcp://DS-W08R2-test:49380			
Application	n URI:				
Security M O None	essage Mode OSign	Sign and Encrypt O None O Basic256 O Basic128Rsa15			

FIGURE 27: MATCH ENCYPTION TO SERVER-SIDE SECURITY

5. Go to the OPC UA Namespace tab to make sure it populates

ASBOPCUAClientService_001					
Genera	al OPC UA	Namespace			
				Refresh	
Index	Alias	Node Id Type	Namespace URI		
	-	and the second se			
0	UA	Integer	http://opcfoundation.org/UA/	1	
0	ALIAS	Integer String	http://opcfoundation.org/UA/ um:DS-W08R2-test:SWToolbox.TOPServer.V5:UA Server		

FIGURE 28: VERIFY NAMESPACE BROWSING

6. Click the **General** tab and assign the platform where this will be deployed, then press **Update**.

3	51	
ASBOPCUAC	lientServi	ce_001
General	OPC UA N	amespace
Scope Name:		TOPServer
		Scope Name will be the Namespace in item references
OPC UA Serve	er Details –	
OPC UA Ser	ver Node:	DS-W08R2-test
Endpoint UR	L:	opc.tcp://DS-W08R2-test:49380
Application U	JRI:	
Security Mes	sage Mode Sign 💽 S	Sign and Encrypt O None O Basic256 O Basic128Rsa15
User Creden	tials	
Anonymo	ous User	
User Name		
Password		
-Service Detail	s	
Port Configu	ration ——	
🔽 Auto-assi	ign port num	ibers
IData Port:		
IBrowse Port	t:	
Assignme	ents	
& 🔽 DS-W08	R2-TEST	
Update	Reset	

FIGURE 29: CHOOSE WHERE OPC UA CLIENT SERVICE WILL BE INSTALLED

7. Save, check-in, and deploy the ASB OPC UA Client Service Instance.

Configure ArchestrA Services							
刘 🔚 刘 🐼 🗙 🔛 🏭 🞫 🧕							
	Service	ASI					
+ 🏭 ASBGRBrowsingS	Save						
ASBMxDataProvic	Rename	F2					
ASBAuthentication	Delete	Delete					
	Export						
	Create Copy						
	Check-out						
	Discard Check-out						
	Check-in						
	Override Check-out	t					
	Save And Check-in						
	Deploy	Ctrl+D					
	UnDeploy	Ctrl+U					

FIGURE 30: SAVE CHANGES

Create a User Defined Object Instance

1. In the IDE, create a User Defined Object (UDO) instance. this Object will be used to read IO data from the OPC server.



FIGURE 31: CREATE A UDO TO READ OPC UA IO DATA

2. Create a field attribute.

Attributes Object Information Scripts	UDAs Extensions	Graphics			
💶+ 🖂+ 🗙	Name:	Analog_001		Attribute type:	Analog
Field attributes:	Access mode:	InputOutput	•	Data type:	Integer
Name	Category:	User writeable	•	Buffered	
Analog_001	Description:				
	-Value 0		- G	Value deadband:	0.0
	Generate ev	ent upon change	a . (%)	Engineering units	• I
	Input source:	,			
	C Output desti	nation differs from	input source		

FIGURE 32: DEFINE A FIELD ATTRIBUTE

- 3. Click the Attribute Browser button next to the Input Source field.
- 4. Choose the Namespace that correlates to your ASB OPC UA Client Service instance and the left panel will populate with the server namespace.



FIGURE 33: CHOOSE THE ASB OPC UA CLIENT SERVICE INSTANCE SCOPE NAME

5. Browse the OPC UA Server namespace and select a tag. Click $\ensuremath{\text{OK}}$.

Instances	Simulation Examples/Functions				
gname 🔺	Attribute A	Data type	Security da		
Data Type Examples/16 Bit Device/S	Simulation Examples.Functions.Ramp1 {Ramp1}	Integer	Free access		
Data Type Examples/8 Bit Device	Simulation Examples.Functions.Ramp2 {Ramp2}	Float	Free access		
Data Type Examples/8 Bit Device/_S	Simulation Examples.Functions.Ramp3 {Ramp3}	Integer	Free access		
Data Type Examples/8 Bit Device/K .	Simulation Examples. Functions. Ramp4 (Ramp4)	Integer	Free access		
Data Type Examples/8 Bit Device/R .	Simulation Examples.Functions.Random1 {Random1}	Integer	Free access		
Data Type Examples/8 Bit Device/S .	Simulation Examples.Functions.Random2 (Random2)	Integer	Free access		
Server	Simulation Examples. Functions. Random3 {Random3}	Integer	Free access		
Server/ServerCapabilities	Simulation Examples.Functions.Random4 (Random4)	Integer	Free access		
Server/ServerCapabilities/Aggregat.	Simulation Examples. Functions. Sine 1 (Sine 1)	Float	Free access		
Server/ServerCapabilities/Modeling.	Simulation Examples. Functions. Sine2 (Sine2)	Float	Free access		
Server/ServerCapabilities/Modeling.	Simulation Examples. Functions. Sine3 (Sine3)	Float	Free access		
Server/ServerCapabilities/Modeling.	Simulation Examples. Functions. Sine4 (Sine4)	Float	Free access		
Server/ServerCapabilities/Modeling.	C Simulation Examples. Functions. User 1 {User 1}	String	Free access		
Server/ServerCapabilities/Modeling.	Simulation Examples. Functions. User2 (User2)	Float	Free access		
Server/ServerDiagnostics	Simulation Examples. Functions. User 3 {User 3}	Boolean	Free access		
Server/ServerDiagnostics/SessionsDi	T Simulation Examples. Functions. User 4 (User 4)	String	Free access		
Server/ServerDiagnostics/SessionsDi					
Server/ServerRedundancy					
Server/VendorServerInfo					
Server/VendorServerInfo/ObjectSta					
Simulation Examples					
Simulation Examples/_Statistics					
Simulation Examples/_System					
Simulation Examples/Functions					
Simulation Examples/Functions/_Sys.					
لغرب	Show all attributes		Property: chippe >		

FIGURE 34: BROWSE THE OPC UA SERVER NAMESPACE

6. Save and Deploy the object. You can now view the tag in Object Viewer.

💋 Object Viewer				
File Edit View Options Help				
) 🎭 🏹 🛤 🗹 🚽	Attribute Reference	UserDefined_001.Ana	alog_001.value	
🖃 💓 test	Attribute Name	Value	Timestamp	Quality
🗄 🖳 WinPlatform_001[DS-W08R	AlarmMostUrgentAcked	true	8/11/2014 10:5.	C0:Good
AppEngine_001	AlarmCntsBySeverity	0,0,0,0	8/11/2014 10:5.	C0:Good
🖻 - 🚯 Area_001 [Area_00	AlarmMostUrgentInAlarm	false	8/11/2014 10:5.	C0:Good
UserDefined_00	Analog_001.Input.ReadStatus	Communication	0/11/2014 10-5	C0:Good
	Analog_001.Input.value	-10 MyInteger	8/11/2014 10:5.	C0:Good
	Analog 001.Input.InputSource	topserver:Simul		C0:Good
	Analog_001	6	8/11/2014 10:5.	C0:Good
	Analog_001.EngUnits			C0:Good
	Analog_001.Bad.Condition	true		C0:Good
	Analog_001.LogDataChangeEver	nt false		C0:Good
	Analog_001.Deadband	0.0		CU:Good
AttributeReference	Value Tin	nestamp	Quality Sta	tus
UserDefined_001.Analog_001	26 8/	11/2014 10:56:17.37	C0:Good Ok	
Watch List 1				
Ready		FILE: User: DefaultUs	er	

FIGURE 35: DEPLOY AND VIEW IO DATA

D. Scott and G. Alldredge

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at Wonderware Technical Support.

For technical support questions, send an e-mail to wwsupport@invensys.com.

Back to top

©2014 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Invensys Systems, Inc. Terms of Use.